Distributed Network Architecture: Scalability and load balancing in a security environment

Global enterprises and large, multi-site hospitals, universities, or government agencies are increasingly facing a common challenge – how to bring all of their disparate buildings into an easy to manage enterprise security system. Most multi-site organisations have a variety of sites, ranging in size from small branch offices to large multi-building campuses. In designing their enterprise security solution, security directors and IT managers focus on the following three priorities:

- // Maintain a single database of all personnel that only needs to be updated once, across all sites
- // Provide both central management and reporting, AND local site control
- // Protect the system and facilities against network failures

Enterprises with different access control software solutions at each site have success with the third priority, but fail the first two. The "enterprise" features of most traditional access control software providers focus on addressing the first priority (common personnel database), but generally fail priorities two and three.

Designing a true enterprise security system that is both easy to use and delivers all three priorities requires access control software that can effectively manage the volumes of data produced by large enterprises via a Distributed Network Architecture. This white paper defines the key elements and benefits of Distributed Network Architecture and describes how Tyco's Software House C•CURE 9000 Enterprise, available with version 2.0, addresses the priorities described above.

Defining enterprise for the purposes of Distributed Network Architecture

According to the Merriam-Webster Online dictionary, an "enterprise" is defined as a company organised for commercial purposes; a business firm. For the purposes of this white paper and to adequately describe Distributed Network Architecture, we will define "enterprise" as a company or organisation consisting of two or more facilities either locally situated or widely dispersed. An enterprise could be multiple facilities grouped together in the same area such as a hospital campus with its main building surrounded by clinics, doctor's offices, etc. Or, it could be a large global company comprised of many buildings hundreds, even thousands of miles apart from each other.

Distributed Network Architecture in today's enterprise environment

The key elements of Distributed Network Architecture are, as the name implies, the distribution of decision-making and control out to each site, while simultaneously, networking and synchronizing the various sites together via a central hub. Distribution of decision-making and control to each site is essential for two reasons. First, local site managers need the flexibility to manage the security needs specific to their site, from adding personnel to modifying access rights, without being dependent on network connectivity and bandwidth back to a central, off-site server. Second, from a scalability perspective, well designed security architecture avoids unnecessary data transmission – adding a new contractor and assigning him/her access privileges at a single local site should not require communication back to a central server. Distributed Network Architecture gives the local sites the information and tools to manage local security decisions autonomously, thereby enhancing the scalability of the system and making it highly tolerant of network failures and bandwidth shortages. "Scalability" in Distributed Network Architecture also refers to the ability to incorporate virtually any size site, from a small sales office with just 4–5 readers to a large office building with thousands of readers.

While local autonomy is essential, security and IT directors demand that this autonomy be combined with powerful central management capabilities via networking and synchronization.

From maintaining a single, global personnel database to ensuring common operating procedures and security clearances across sites, successful enterprise architecture must also give the managers responsible for the entire enterprise the ability to define and change rules, records, and privileges once, and ensure they are instantly shared across all sites of the enterprise. The multiple autonomous servers at each site can be in communication with the central hub via either a Local Area Network (LAN) or Wide Area Network (WAN).

Synchronization refers to the ability to enter or change data at one of the local sites, or the central hub and have that information shared across all of the sites of the enterprise.

The benefits of **Distributed Network Architecture** are clear:

// **Scalability:** Enterprise solutions that rely on a single enterprise server inevitably suffer from performance issues as the enterprise grows and the server is overwhelmed. Moreover, single server solutions are highly susceptible to network failures.

// **Efficiency:** Security managers control the flow of data and decision-making. Local data and decisions can be transmitted to each individual site, minimizing network bandwidth, and allowing global managers to focus on truly global issues. At the same time, centrally located global managers can easily run reports, make changes, and view the status of local sites without needing to login to multiple separate systems.

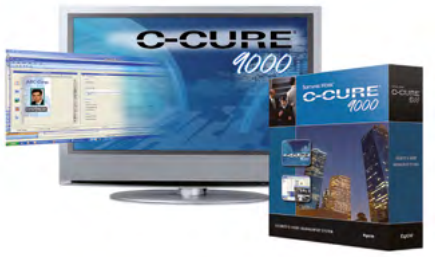
// **Cost:** Servers and software at each local site can be appropriately sized to meet the specific needs of each site, without requiring the installation of an expensive server at even the smallest sites.

// **Reliability:** Distributed Network Architecture is much more tolerant of network and hardware failures than a single server approach.

These benefits can be made clear with a simple use case – a large organisation wants to integrate their access control system with their ERP system to eliminate replication and redundancy of employee data. With a distributed, but not networked, architecture using separate standalone access control solutions, the organisation needs to pay for and maintain multiple separate ERP integrations to the access control software at each local site.

With a networked, but not distributed architecture (the classic, single server approach), only one integration is required but system performance is poor at local sites and network bandwidth consumption is high. Distributed Network Architecture offers a single, cohesive solution that allows for a single ERP integration and optimised system performance and network bandwidth.

C•CURE 9000 Enterprise: The answer to efficient enterprise scalability



C•CURE 9000 Enterprise, available with C•CURE 9000 version 2.0, is a Windows-based system, comprised of a master application server (host) and database, which communicates with several regional sub-systems, known as satellite application servers. C•CURE 9000 Enterprise gives corporate security personnel and IT managers central control over the entire system which could span many facilities across geographical areas, while each local facility maintains independent control of its individual operation. C•CURE 9000 Enterprise also allows system administrators at the main facility to configure and monitor all locations from a single site.

Each local server can be positioned on an independent LAN along with assigned access control hardware such as iSTAR door controllers, readers, door locks, etc. This configuration helps to manage network traffic while optimizing performance of the system. Each local server maintains a local SQL database which increases system reliability as well as reducing network traffic since there is no dependence on the master database or WAN (such as the Internet) connection for normal operations. Local servers manage all mission critical database functions locally as well as supporting 3rd party (video, intrusion, etc) integrations at the site.

Data from each local server is synchronised with the master database via the WAN to ensure data consistency. All database information, including badge holder records, access privileges and controller/reader configuration information is sent to the central server.

In addition, when updates to global information are made on the main server, those updates are distributed to the various local satellite servers to ensure local data is current.

The C•CURE 9000 Enterprise system allows operators to monitor alarms from one, many, or all satellite application servers simultaneously from one client workstation connected to the master application server. You can accomplish this by simply choosing which satellite servers to interactively monitor. A global journal and audit report can be created at the main facility for consolidated tracking of personnel or event information. Journal and audit data is synchronised from the satellite application servers to the master application server by schedule or events. Once synchronised to the master application server, these reports can be used for internal investigations or to comply with company mandates. Even prior to synchronization of the journal and audit data, all information is accessible from the master application server administration client.

Summary

Distributed Network Architecture solves the hardware performance, regional WAN scalability, and load balancing issues inherent in single-server architecture. Distributed Network Architecture can effectively perform on both a small and enterprise scale that allows the flexibility of either central or distributed control.

About Software House

Software House, part of Tyco Security Products, manufactures security and event management systems including the innovative C•CURE 9000. Combined with a suite of reliable controllers led by the iSTAR Edge IP door control module, Software House technologies are among the most powerful in the industry. Add an unsurpassed integration platform that allows customers to integrate seamlessly with critical business applications, and

it's easy to see why Software House solutions are ideal for security-critical applications.

Tyco Security Products, a business unit of Tyco International, is a unified group of world-leading access control, video and intrusion brands. Operating in more than 40 offices with over 2.000 employees, these brands- American Dynamics, Bentel, CEM Systems, DSC, Kantech, Software House, CONNECT24 and Sur-Gard- have more combined years of experience in the security industry than any other group in the world.

Our security integration platforms, built by our developers from across all product disciplines allow our customers to see more, do more, and save more.

Our solutions today are designed to be compatible with the technology of tomorrow.

For further information please contact: ce.communications@tycoint.com or visit our website: www.tyco.eu